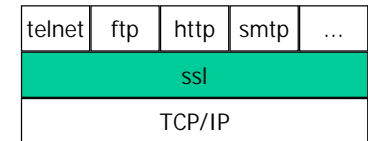


Secure Socket Layer

Giorgio Valent (SSGRR) giorgio.valent@ssgrr.it

Sicurezza del trasferimento di dati: SSL

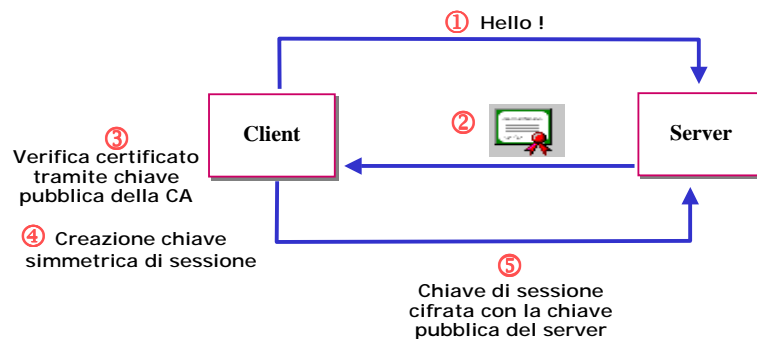
- Secure Socket Layer
 - Sviluppato da Netscape Communication
 - Sostituisce l'interfaccia socket (tra la rete e le applicazioni)
 - Supporta qualsiasi applicazione (HTTP, FTP, ...)
 - In HTTP individuato da URL del tipo https://... (port 443)
- Garantisce
 - riservatezza
 - autenticazione
 - integrità
- Si basa su
 - SSL Handshake Protocol
 - SSL Record Protocol



SSL Handshake Protocol

Per aprire una sessione tra server e client è necessario

- Autenticare gli end-point
 - Certificati X.509
 - Pre-shared secret
- Concordare gli algoritmi (di cifratura, autenticazione ed integrità)
- Concordare le chiavi
- ...



SSL Record Protocol

- Consente di incapsulare dati e informazioni di autenticazione
- I messaggi SSL sono accorpati in record lunghi fino a 32.767 byte

